



Session 6

Information Security & Identity Theft

Chris Aidan

IT Security Manager
Pearson Technology

Matt Wardle

Special Agent
Office of Inspector General

Kristen Frias

Special Agent
Office of Inspector General



Topics Covered

- Internet Dangers
- Identity Theft
- Social Engineering
- Password Selection
- Email & Chat Services
- Securing Workstations
- Data Backups
- Equipment Disposal
- Data Disposal
- Administrative Accounts
- Physical Security
- Latest Threats
- Creating Awareness
- Legislation
- Questions



Identity Theft

What it is and how to avoid it

**Acquisition of key personal
information used to impersonate
someone else**

One of the fastest growing crimes in the
United States



Keeping Your Information Private

Protect Your Information:

- Date of Birth
- Social Security Number
- Drivers license number
- Passwords and PIN's
- Banking Information



Common Identity Theft Practices

- Obtain or take over financial accounts
- Open new lines of credit
- Take out loans for large purchases
- Sign lease agreements
- Establish services with utility companies
- Write fraudulent checks
- Purchase goods and services on the Internet



Avoiding Identity Theft

Don't carry your SSN card with you

- Request a drivers license number
- Shred sensitive information
- Only carry what you use
- Photo copy all cards in your wallet
- Select hard to guess PINs and passwords
- Don't leave mail sitting in an unprotected box
- Don't give out private information over the phone
- Order your credit reports
- Use caution when providing ANY sensitive information



Protecting Others From Identity Theft

- Properly handle documents
- Shred sensitive information
- Use key identifiers instead of the SSN
- Password protect sensitive information
- Audit access
- Review access privileges
- Verify who you are talking to



U.S. Department of Education Office of Inspector General





Examples of ED Identity Theft Investigations

- **Agencies:** ED, SSA, United States Secret Service
- **Loss:** \$300,000
- 1 defendant who used approximately 50 identities of prison inmates to get financial aid
- Examples of additional identity theft cases



U.S. Department of Education Background

- ED disburses approximately **\$52 Billion** Per Year in educational program funding.
- **7500** domestic and international universities/colleges participate in DoED financial aid programs.
- During this year, approximately **12.6 million** Students will apply for Federal Student Financial Aid.
- **9 million** will apply electronically via the internet.



Student Financial Aid Demographics

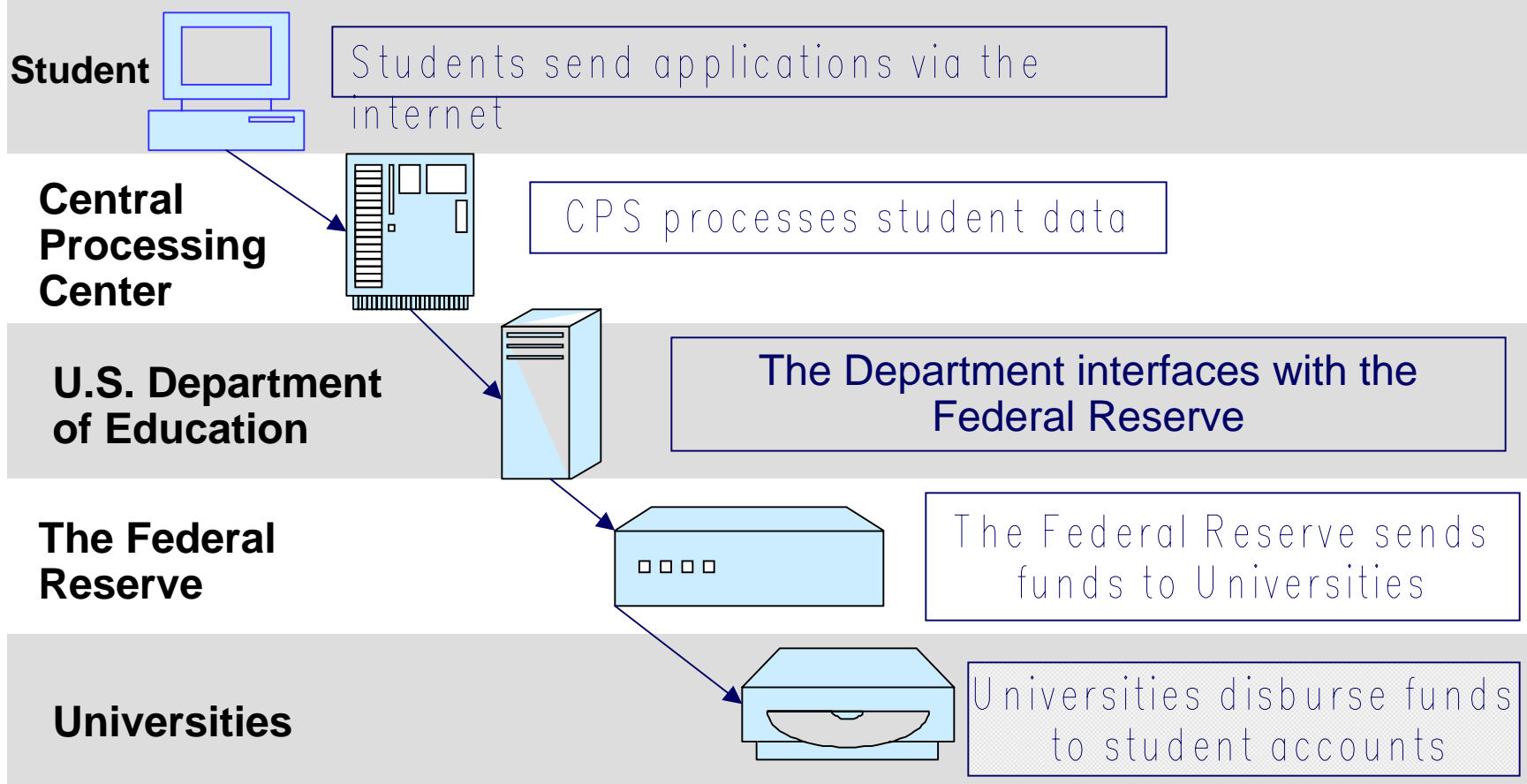
Student Aid is Disbursed World Wide

- 58 US States and Territories
- 41 International Countries





ED Funds Infrastructure





OIG Identity Theft Program Goals

- Consumer Awareness Campaign
- Hotline Set-up
- Data Mining
- Investigate Referrals
- Coordination with other Agencies



President Bush and
Secretary Roderick Paige



Consumer Awareness Campaign

- Information to be posted on ED WebPages, Handbooks and Posters.
- Case Summaries to be sent to school e-mail-presentation to schools
- Prepackaged case reports to College papers
- Presentations to Professional Groups.
- Employee Awareness Efforts.





Hotline

“1 800 MIS-USED”

“Oig.hotline@ed.gov”

- ED Customer Awareness Campaign for identity theft. The website can be access at:
<http://www.ed.gov/misused>
- Boston Region referrals-contact (617) 223-9301
- New York Region referrals-contact (212) 264-4104





Data Mining



- ED/SSA Death Records Match
- Similar Applicant Addresses
- Similar SSN/DOB





What You Can Do as a Financial Aid Officer

- When verifying identity documents, ask to see originals (original social security cards, birth certificates, etc)
- If a document appears suspicious request additional forms of identity (white out, altered, original not available)
- Make referrals to the US Department of Education Office of Inspector General



SAR Comment Codes

- Pay Attention to SAR Comment Codes as a Fraud Indicator
 - #060: Date of Birth does not match SSN
 - #061: Name does not match SSN
 - #062: Citizenship Status does not match
 - #063: Date of Birth does not match SSN
 - #064: Name does not match SSN

When in doubt ask to see original documents!



Sources of Referrals

- Financial Aid Professionals at schools
- Calls from Citizens
- Other law enforcement agencies
- Proactive Projects





Liaison/ Coordination

FTC



USPS



SSA-OIG



USSS



USAO



Passwords

- Know how to select a good one
 - At least 7 characters
 - Mixture of upper and lowercase characters
 - Mixture of alpha and numeric characters
 - Don't use words you can find in a dictionary
- Keep passwords safe
- Change them often
- Don't share or reuse them



Password Selection Tips

- Everyday items can make great passwords:

1/4#Burger 2004EACno Onmy30thBday

Use simple sayings, poems or songs

I like to go to go to the Electronic Access Conference **il2g2tEAC**

The bus stops near my campus at half past four **Tbsnmc@1/2p4**

TIGER, tiger, burning bright In the forests of the night, **Ttbbittfotn,**

Dear Prudence, wont you come out to play **DP,wyco2p**

Passwords to Avoid:

- | | |
|--------------------|-----------------------------------------------------|
| – Names | – Places |
| – Computer Name | – Months/Dates |
| – Phone numbers | – Repeated letters (e.g. "xxxxxxx") |
| – SSN | – Keyboard patterns (e.g. "qwerty", "zxcvbn", etc.) |
| – DOB | |
| – Usernames | |
| – Dictionary words | |



Social Engineering

Social Engineering is the art of prying information out of someone else to obtain access or gain important details about a particular system through the use of deception



Email & Chat Services

- Email and chat are sent in clear text over the Internet
- Data can easily be captured and read by savvy computer users and systems administrators
- Safeguards should be put into place prior to using these programs for sending/receiving sensitive information like Social Security Numbers



Securing your Workstations

- Lock your system
- Shut down
- Run Virus Scanning Software
- Password Protect Files
- Apply Patches



Is Your Data Being Backed Up?

- Test your backups
- Securely store backup media
- Restrict Access



Equipment Disposal

- What happens to your old systems when they are replaced?
- Do those systems contain sensitive information?
- A recent MIT study displayed the importance of proper computer disposal
- Several programs to securely remove data from computer systems are commercially available



Dumpster Diving

- You never know who is looking in your trash
- Shred sensitive documents
- Secure your shred barrels, and make sure that proper handling procedures are in place.
- Secure all trash in secure bins when possible



Administrative Accounts

- Only allow access that is absolutely required
- Don't grant accounts based on the fact that access "may" be required
- Use least privilege access policies that state access will only be granted if required, not by default.
- Are accounts removed and passwords changed when someone changes jobs or is terminated?



Physical Security

- Who has access to your computer systems when you're not there?
- Are sensitive documents secured when not in use? (clean desk policy)



Latest Types of Threats

- Wireless Technology
- Memory Devices
- Camera phones
- P2P File Sharing



Creating Awareness

- Educate your staff
 - Train your staff
- Research candidates
 - Perform background & credit checks
- Track changes
 - Audit system access
 - Audit system changes
- Create Policies:
 - Define document and system disposal processes
 - Define backup procedures
 - Define clean work area policies
 - Define computer usage policies



Legislation

- Identity Theft Victims Assistance Act of 2002-Bill 1742
- Identity Theft Prevention Act of 2001-S.1399
- Identity Theft Assumption & Deterrence Act of 1998
- Privacy Act
- Computer Security Act of 1987
- Computer Fraud And Abuse Act
- Electronic Communications Privacy Act of 1986
- 2001 USA Patriot Act
- Gramm-Leach Bliley Act (GLBA) (required by May 23, 2003)
- California SB 1386
- Family Education Rights & Privacy Act (FERPA)
- Health Insurance Portability and Accountability Act (HIPAA)



Fraud Contact Information

Office of the Inspector General

1-800 MIS-USED (647-8733)

Email: Oig.hotline@ed.gov

Social Security Administration, Fraud Hotline

1-800-269-0271

Federal Trade Commission

1-877-IDTHEFT (438-4338)

Equifax Credit Bureau, Fraud

1-800-525-6285

Experian Information Solutions

1-888-397-3742

TransUnion Credit Bureau, Fraud

1-800-680-7289



Credit Bureau Contact Information

Experian

<http://www.experian.com>

P.O. Box 949

Allen, TX 75013-0949

Telephone:

1-800-397-3742

TransUnion

<http://www.tuc.com>

P.O. Box 1000

Chester, PA 19022

Telephone: 1-800-916-8800

Equifax

<http://www.equifax.com>

P.O. Box 740241

Atlanta, GA 30374-0241

Telephone:

1-800-685-1111



Be Aware

- Report anything that you think is strange
- Don't give private information out unless you know who you are speaking with and you initiated the call
- Properly dispose of sensitive information
- Run up to date virus protection
- Ask questions, don't take anything at face value



Useful Links

For additional information on the GLBA, see the FTC's site at:

<http://www.ftc.gov/privacy/glbact/>

National Institute of Standards and Technology:

<http://csrc.nist.gov/sec-cert/>

Office of the Inspector General

<http://www.ed.gov/about/offices/list/oig/index.html>

A lot of Schools have great security resource pages, for example
UC Davis and the University of Iowa websites:

<http://security.ucdavis.edu/security101.cfm>

<http://cio.uiowa.edu/itsecurity/>



Questions?

New law passed before Thanksgiving adds new consumer protections:

- Home mortgage applicants will automatically receive a copy of their credit score.
- Credit reporting agencies must fix erroneous information blamed on identity theft within four business days of receiving a police report, and must inform the creditor who generated the inaccurate information.
- The right for victims to get application and transaction data from firms that extended credit to identity imposters. This provision helps victims who often find they must do their own investigations before they can interest law enforcement in their case.
- Several measures designed to stop identity thieves from obtaining more credit using a victim's information once a victim reports the ongoing crime to authorities.

Please fill out the session evaluations & thank you for attending this session



Technical Assistance

We appreciate your feedback and comments.
We can be reached at:

Chris Adain

Phone: 319- 339-6619

Email: Chris.Aidan@Pearson.com

Special Agent Matt Wardle

Phone: 617-223-9301

Fax: 617-223-4109

Email: Matt.Wardle@ed.gov

Special Agent Kristen Frias

Phone: 212-264-4104

Fax: 212-637-0603

Email: Kristen.Frias@ed.gov